



Argentina \$ 22.- // México \$ 49.-

Técnico en

REDES & SEGURIDAD

24

CÁMARAS IP

En esta clase conoceremos el funcionamiento y las ventajas de las cámaras IP, además de sus diferencias con un circuito cerrado de TV. Veremos la forma en que debemos configurarlas para monitorear las instalaciones donde se encuentran localizadas.

- ▶ TIPOS DE CÁMARAS
- ▶ INSTALACIÓN FÍSICA
- ▶ CONFIGURACIÓN AVANZADA
- ▶ DETECCIÓN DE MOVIMIENTO
- ▶ ADMINISTRACIÓN LOCAL Y REMOTA



USERS

Técnico en **REDES** & SEGURIDAD

Coordinador editorial

Paula Budris

Asesores técnicos

Federico Pacheco

Javier Richarte

Nuestros expertos

José Bustos

Gustavo Cardelle

Rodrigo Chávez

Santiago Crocioni

Alejandro Gómez

Gilberto González

Javier Medina

Gustavo Martín Moglie

Juan Ortiz

Pablo Pagani

Gerardo Pedraza

Marcelo Soria

Curso visual y práctico Técnico en redes y seguridad es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Copyright © Fox Andina S.A. I, MMXIII.

Revista
POWER
TODA LA POTENCIA
DE TU PC
BAJO CONTROL

También Digital



usershop.redusers.com
+54 (011) 4110-8700
✉ **USERSHOP@REDUSERS.COM**
Recorré parte de la revista en  **redusers.com**

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Características generales y funcionamiento de las cámaras IP. También conoceremos la forma adecuada de instalarlas y configurar sus opciones básicas y avanzadas.



En la clase anterior conocimos los detalles de la telefonía IP, vimos el estándar VoIP, conocimos el funcionamiento de una central telefónica y revisamos las características de la plataforma FreeSWITCH. Para continuar, analizamos las ventajas de Cisco Unified Communications Manager y profundizamos en la seguridad relacionada con VoIP. Para terminar, vimos qué es un ataque de vishing, cuáles son los principales problemas que podría ocasionar y de qué forma debemos protegernos; también analizamos el ruido de fondo de Internet y sus posibles causas. En esta clase, veremos el funcionamiento y los tipos de cámaras IP existentes, y aprenderemos a configurar una cámara IP tanto en sus opciones básicas como en las opciones avanzadas. Para continuar, aprenderemos a instalar una cámara en forma física y configuraremos el router para permitir el monitoreo. Por último, veremos cómo administrar una cámara IP en forma local y remota, configuraremos la detección de movimiento y entregaremos importantes consejos sobre la seguridad relacionada con estos dispositivos.



24

2

Cómo funciona una cámara IP

14

Administración de cámaras IP

16

Configuración adicional de cámaras IP

22

Seguridad y cámaras de monitoreo



Cómo funciona una cámara IP

En estas páginas, conoceremos en detalle las características de hardware y el funcionamiento general de las cámaras IP así como también los principales usos que nos ofrecen.

Las cámaras IP surgen de la necesidad de querer tener supervisadas, o vigiladas, zonas de nuestra propiedad en cualquier momento, incluso cuando no nos encontremos allí; también, si alguien llama a nuestra puerta, podríamos ver de quién se trata desde algún lugar de nuestro hogar sin necesidad de acercarnos a ella.

Cámaras de seguridad

Al principio, el monitoreo de lugares físicos a través de cámaras de seguridad estaba limitado a las empresas o grandes comercios debido a sus altos costos. Este sistema es conocido como **Circuito Cerrado de TV (CCTV)**, en el que todas las cámaras de vigilancia se conectaban a un equipo central y este a un monitor que es observado y manejado por personal de seguridad contratado, que se encarga de visualizar las cámaras y alertar a otros en caso de notar algún hecho, generalmente delictivo o que dañe propiedad de la



El print server de Encore permite realizar la conexión de casi cualquier dispositivo USB, incluso de cámaras web, y, con un replicador de puertos, podemos conectar hasta cuatro cámaras web.



Software adicional

No es obligatorio utilizar el software original que puede incluir la cámara que adquirimos. Hay varias alternativas, incluso gratuitas, con numerosas funciones, para visualizar las cámaras desde nuestra PC o tablet. Algunos programas que están diseñados exclusivamente para equipos móviles nos permiten la visualización en simultáneo de hasta cuatro cámaras; uno de ellos es **IP Cam View Lite**.



empresa. Las primeras cámaras utilizadas en los sistemas CCTV solo mostraban imágenes en blanco y negro; sus conexiones se realizaban mediante cables **RCA** o también **Coaxial**.

LAS CÁMARAS IP NOS PERMITEN VISUALIZAR LUGARES REMOTOS DESDE LA PC, UNA TABLET O UN SMARTPHONE.

Adaptación

Los usuarios domésticos que querían poseer cámaras de seguridad, adaptaban sus cámaras web, utilizando distintos cables como alargue para el **cable USB**. Esta forma tenía sus limitaciones: había que dejar la PC prendida todo el tiempo para su visualización o grabación; no se podía acceder a la cámara directamente, solo podía hacerse desde la PC que tenía instalada la cámara web y, según el tipo de webcam, al tener una modificación en su cable USB, era muy probable que fallara. También podemos utilizar algunos **print server**, que tienen conexión USB y Ethernet; con ello, no tendremos que modificar el cable original de nuestra cámara y obtenemos una gran distancia al ser el cableado por **UTP**. Como fue un método muy utilizado por los aficionados, surgieron software que permiten utilizar nuestra cámara web como cámara de seguridad; uno de ellos es la aplicación **Vitamin D** (www.vitamindinc.com), que grabará únicamente cuando detecte movimiento en la zona que está siendo vigilada.

Funcionamiento

El funcionamiento de las **cámaras IP** se puede considerar como una mezcla entre las cámaras de CCTV y las webcam. Están diseñadas para poder conectarse a través de cables de larga distancia sin perder calidad de imagen, y, en algunos casos, incluyen audio. Podemos conectar varias cámaras IP a una misma PC, y, utilizando software para monitoreo, es posible visualizar varias cámaras al mismo tiempo.

El funcionamiento interno es sencillo y se puede comparar, en cierto modo, al de las cámaras de fotos, ya que procesa imágenes; en la cámara de fotos, estas imágenes son almacenadas en su memoria, mientras que en las cámaras de seguridad son enviadas al receptor, que es un monitor externo y alejado de donde se encuentran las cámaras IP. En su interior, poseen una lente, que puede ser un lente genérico fijo de pocos megapíxeles o incluso **VGA** (0,3 MP), y, según su calidad, podremos visualizar la imagen con mayor o menor nitidez. Las cámaras IP de seguridad profesionales poseen lentes intercambiables de gran precisión que se pueden ajustar según la distancia a la que se encuentren, incluso con visión nocturna. Esta lente está montada a través de conectores o soldada a una placa lógica, que posee conexión Ethernet, y el jack para la alimentación eléctrica. La mayoría de las cámaras incluyen un pequeño micrófono, y algunas pueden tener salida de audio. En esta salida de audio, irán conectados unos parlantes que reproducirán lo que nosotros digamos desde el micrófono de nuestra PC, y, a través del micrófono que está en la misma cámara, podemos interactuar con la o las personas que estemos observando. Además de la conexión Ethernet, incluyen conexión wireless; aunque visualmente no podamos distinguir su antena, es muy probable que cuenten con ella. Todos estos datos son procesados en forma digital por la placa lógica de la cámara y enviados a través de la conexión Ethernet o Wi-Fi.

Hardware

A nivel hardware, la lente permite el paso de la luz hacia el sensor. Los sensores **CMOS** y **CCD** (*Charged-coupled Device*, que en español significa dispositivo de carga acoplada) son circuitos eléctricos compuestos por varios capacitores acoplados, llamados células fotoeléctricas. La resolución máxima a la que se puede obtener una imagen coincide con la cantidad de células que posee el sensor, o sea que la resolución máxima de una fotografía o video no solo está determinada por la lente, sino directamente por el sensor. En la actualidad, encontramos modelos con un tipo de sensor u otro; si bien el funcionamiento es similar, el



Las cámaras web se pueden conseguir en varios modelos, y su uso como cámara de seguridad puede pasar desapercibida.

sensor CMOS permite tomar fotografías por ráfagas, lo que lo hace ideal para la grabación de video de alta definición. Este sensor recibe la luz proveniente de la lente y, por efecto fotoeléctrico, genera una corriente por cada célula, que será procesada para generar la imagen.

Software

Algunos fabricantes incluyen con sus cámaras software específico para poder visualizarlas. La ventaja que tiene la utilización del software reside no solo en que contaremos con opciones de grabación, sino que, si decidimos agregar más cámaras del mismo fabricante, podremos visualizar, en forma simultánea, todas las cámaras que tengamos instaladas, construyendo un CCTV. Esto proporciona la escalabilidad del sistema. Las cámaras IP no requieren drivers para la visualización desde la PC, tablet o smartphone y, comparadas con el viejo sistema de CCTV, poseen la ventaja, hasta cierto punto, de ser una solución más económica, de fácil manejo y reemplazo; comparadas con el nuevo sistema CCTV, es una alternativa económica. Su elección dependerá de nuestras necesidades. ■



Tipos de cámaras IP

Las características y las funcionalidades de los distintos modelos de cámaras IP serán analizadas en detalle en estas páginas.

Los fabricantes de cámaras IP nos proveen de varios modelos que pueden ajustarse a nuestras necesidades; por esa razón, es posible encontrar cámaras de muy alto valor, y otras convencionales; su elección dependerá de dónde las ubicaremos. Por ejemplo, una institución bancaria requerirá un complejo sistema de seguridad con cámaras ultrasensibles; en cambio, en nuestro hogar no necesitaremos una cámara con grandes prestaciones.

Cámaras analógicas

Este tipo de cámara no es IP, y su conexión se realiza a través de cableado coaxial o con conectores RCA, lo que hace que se requiera de un cableado desde la posición de la cámara hasta una PC que tenga placa sintonizadora con entrada RCA, o un pequeño televisor. Los modelos y características de cámaras varían tanto como las IP. Las más básicas poseen conector RCA, y según su tamaño físico, algunas no requieren una alimentación de corriente externa, ya están listas para transmitir la imagen directo al televisor. La ventaja de este tipo de cámara es su diminuto tamaño, que permite ubicarla o esconderla en cualquier lugar. Las cámaras que utilizan conexión por cable coaxial, usadas en CCTV, se deben conectar a un equipo central, y este, a su vez, se conectará a un monitor para su visualización. Estas cámaras poseen lentes removibles, lo que permite adaptarlas fácilmente con funciones de visión nocturna, con solo reemplazar su lente. Debemos tener en cuenta que también, existe hardware que es capaz de convertir la señal analógica entregada por las cámaras, para que sea enviada sin inconvenientes a través de una red Ethernet.

Cámara IP estándar

Este tipo de cámara tiene conexión Ethernet, y opcionalmente con wireless. Debido a la poca diferencia económica, ya es común que incluyan ambas conexiones de red. Poseen un lente fijo de baja resolución, lo que no la hace apta para visualizar lugares abiertos o con mucha intensidad de luz solar; en cambio podemos utilizarla en espacios reducidos, como pequeñas oficinas. Posee dos ajustes a presión para establecer la mejor posición de acuerdo a su ubicación física.

LAS CÁMARAS ANALÓGICAS SIGUEN UTILIZÁNDOSE CON SISTEMAS MODERNOS DE MONITOREO, COMO LOS NVR.

Cámara IP con visibilidad nocturna

Este tipo de cámaras traen un conjunto de **led fotosensible** alrededor de la lente, que se activa en forma gradual según la menor intensidad de luz que haya en el ambiente. Pueden utilizarse en ambientes exteriores si se toman ciertas precauciones para evitar daños por lluvias, etc. La desventaja que poseen las cámaras genéricas con visión nocturna reside en que, en ambientes totalmente oscuros, los leds de la lente que se iluminan la hacen fácilmente detectable a varios metros de distancia. Se pueden configurar para que, al captar movimiento en una zona que hayamos configurado como sensible, tomen fotografías y las reenvíen por correo electrónico.



Sistema NVR; permite conectar dispositivos como cámaras, monitor o TV, y Ethernet.

Modelo de cámara IP que suele ser utilizado para los DVR o NVR.



Cámara IP PTZ

Su nombre proviene de **Pan Tilt Zoom**. También se las suele conocer con el nombre de Cámara Domo. Además de contener las ventajas de las dos cámaras anteriores, estas incluyen un mecanismo que puede rotar su posición y, así, conseguir un mayor grado visual. Poseen un mecanismo que permite rotar horizontalmente (*panning*), otro verticalmente (*tilt*), y hacer zoom a una determinada área. Algunas cámaras incluyen la función de autoseguimiento, que es similar a la detección por movimiento, solo que, en este caso, la cámara rotará en forma automática siguiendo la fuente en movimiento. Todos sus controles para el movimiento pueden realizarse desde el mismo navegador en el que visualizamos nuestra cámara IP PTZ.

Este tipo de cámara no posee ajustes a presión para colocarla, y, como viene todo en conjunto debido a su mecanismo de rotación, si decidiéramos colocarla en una pared o un techo, tendríamos que configurar su visualización para que nos permitiera rotar la imagen que vemos. En la parte posterior, posee cuatro conectores que podremos utilizar para conectar un relé que activará luces, y un sensor de movimiento adicional, para complementar las funcionalidades de la cámara.

Sistemas DVR/NVR

Son equipos para vigilancia centralizada; en este caso, todas las cámaras de un lugar se conectarán a este equipo. Las siglas provienen de *Device Video Recorder* y *Network Video Recorder*. El aislado **sistema CCTV** que utiliza cámaras analógicas con conexión por cable coaxial y con cintas magnéticas para su grabación quedó desplazado por el DVR que emplea discos duros para esa misma función; además de simplificar la tarea a través de su configuración interna, podemos establecer el tiempo que deben permanecer las filmaciones guardadas y de qué cámaras se necesitan grabaciones continuas las 24 horas. El **NVR** utiliza cámaras IP para todo su conjunto; estas se conectarán por cable Ethernet o wireless al NVR, que, además de incluir las funciones del DVR, tiene conexión a Ethernet directa para el router, con lo cual podremos visualizar todas las cámaras desde cualquier puesto de la red o desde Internet. El NDVR es un híbrido entre ambas; puede aceptar conexión de cámaras analógicas o IP y tiene conexión propia a Ethernet

para poder visualizarlas en forma remota. Al aceptar los dos tipos de cámaras, lo convierte en un producto ideal para adaptar el sistema CCTV a la actualidad sin demasiados cambios en la estructura general del sistema de seguridad. Todos estos sistemas permiten la conexión simultánea de 4, 8 o 16 cámaras; poseen un sistema operativo Linux adaptado para tal fin. Se puede configurar que las grabaciones se guarden en un disco duro externo (ftp interno). Durante su configuración, se nos pedirá crear un mínimo de dos usuarios: un usuario administrador, con el cual configuraremos la hora, las grabaciones, el acceso remoto, o borrar contenido manualmente; y un usuario básico, que solo podrá visualizar las cámaras. Podemos crear más de un usuario básico y darle determinados permisos para la configuración del NVR. ■



Cámara IP hogareña; aunque no podamos ver su antena, posee conexión Wi-Fi.

Tipos de lentes

Para seleccionar el tipo de lente, que se mide en milímetros (mm), nos basaremos en la distancia horizontal o vertical que deseamos cubrir y en la distancia desde la cámara al objetivo. Para un sensor de 1/3" CCD, tenemos los datos de fábrica de la distancia focal (distancia del lente al sensor), usaremos $h'=4,8\text{mm}$ y $v'=3,6\text{mm}$, que son valores que utilizaremos para calcular el tamaño de la lente según la distancia y el foco de visión horizontal o vertical que deseamos cubrir. Llamaremos D a la distancia desde la cámara hasta el objetivo, V a la distancia vertical y H a la distancia horizontal que deseamos visualizar.



Configuración inicial de una cámara IP

La configuración inicial de una cámara IP es una tarea sencilla, pero requiere que tengamos en cuenta algunos pasos importantes.

1



2

How to Access the Web-based Utility

To access the Utility, launch Internet Explorer, and enter the Camera's IP address in the Address field. IP address is **192.168.1.115**. Then press **Enter**.

The **Welcome** screen of the Web-based Utility will appear.

You have six tabs available:

- **Home**. To return to the **Welcome** screen, click the **Home** tab.
- **View Video**. To view the Camera's video, click the **View Video** tab. Go to the "View Video" section for information.
- **Setup**. To alter the Camera's settings, click the **Setup** tab. Go to the "Setup" section for more information.

3



4



1

Para su configuración, debemos conectar la cámara a través de su puerto Ethernet directo a la PC. Si la PC se encuentra conectada al router, desconectaremos el cable del router. Aunque nuestro router tenga bocas disponibles, igual lo debemos conectar por primera vez directo a la PC.

2

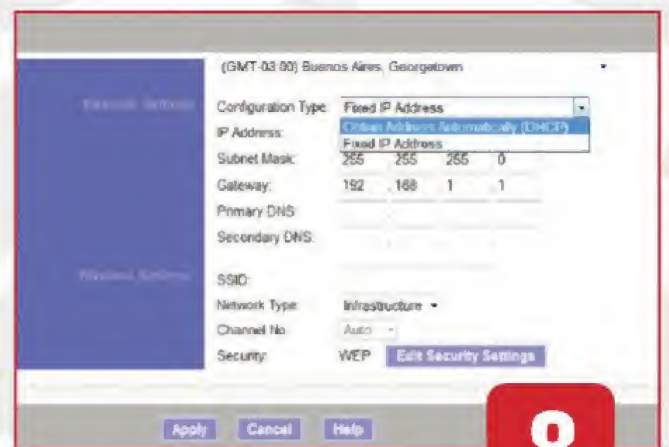
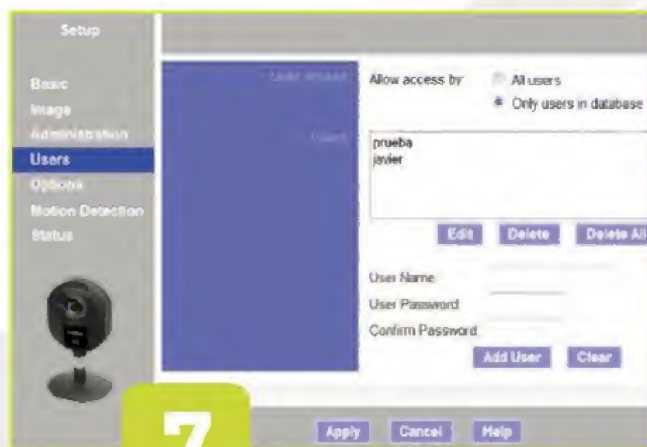
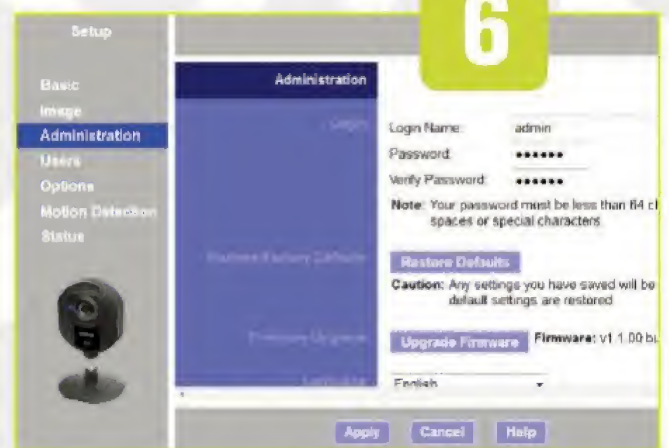
De la misma forma que el router trae una IP fija de fábrica, la cámara IP también tiene una IP preestablecida. Para encontrar la IP, busquemos una etiqueta en la cámara o leamos el manual. Debemos configurar la IP de la PC para que se encuentre en la misma red.

3

Al ingresar esa dirección IP en nuestro navegador de Internet, veremos la página principal de nuestra cámara IP. Para visualizarla y, también configurarla, se nos pedirá un nombre de usuario y contraseña. Debemos buscar esta información en el manual.

4

Podemos ingresar un nombre a la cámara, su descripción, y cambiar la IP, desde la configuración básica. Si vamos a instalar varias cámaras, es conveniente que el nombre de cada una se relacione con la ubicación que va a tener.



5 En este apartado configuraremos la calidad que deseamos obtener de la cámara, elegimos entre los formatos MPEG, MJPEG, y modificamos la cantidad de FPS. Recordemos que a mayor cantidad de FPS, mayor tráfico de la red. Dependiendo de la ubicación de la cámara, configuraremos qué calidad deseamos obtener.

6 En la sección de administración, configuraremos el usuario **admin**. Podemos utilizar el mismo nombre de usuario o cambiarlo por otro. Es aconsejable modificar todos los parámetros que vienen por defecto en la configuración de la cámara. Una vez aceptados estos cambios, podemos conectar la PC.

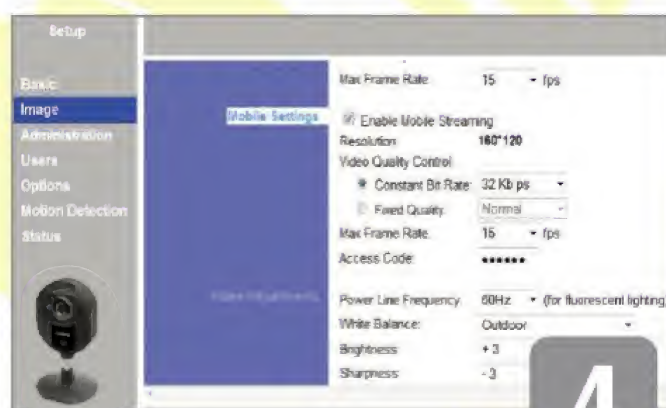
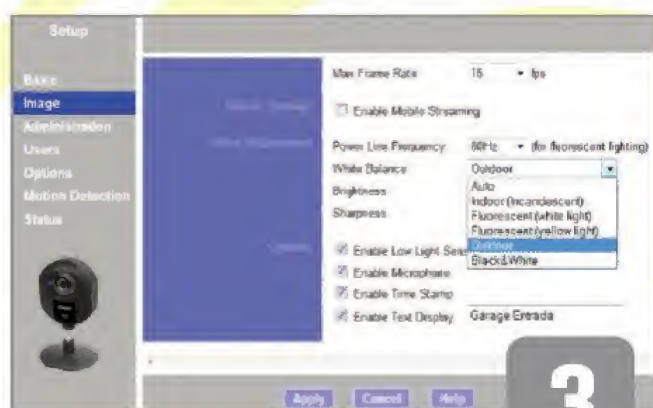
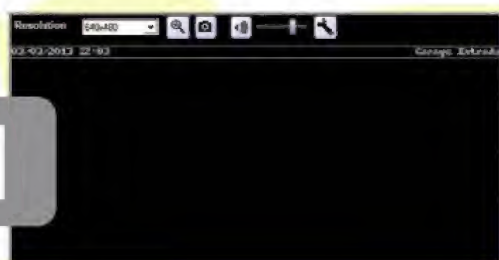
7 En la sección de usuarios, podemos agregar todos los usuarios que deseamos que solo tengan acceso visual a la cámara. Es decir, estos usuarios podrán ver la imagen de la cámara desde cualquier punto de la red, pero no podrán realizar ninguna modificación en ella, ni siquiera cambiar su password.

8 Al configurar la IP de la cámara, esta debe estar dentro del rango de nuestra red, para que luego, al conectarla al router, podamos acceder a ella desde cualquier ubicación. No conviene usar DHCP para la configuración de la cámara.



Configuración avanzada de una cámara IP

En esta sección, revisaremos en detalle el proceso de configuración avanzada de una cámara IP.

**1**

Algunas cámaras IP, nos permitirán manejar el brillo, el volumen o tomar una instantánea, a través de un control que se posiciona arriba de la imagen visualizada. Este control se activará luego de instalarse un complemento OCX para Internet Explorer. Si utilizamos otro explorador web, es probable que estos controles no aparezcan.

2

Para configurar la conexión wireless, nos permitirá elegir, desde el menú Wi-Fi, las conexiones que la cámara detecte cercanas. En la mayoría de los casos, deberemos ingresar manualmente todos los parámetros de nuestro router Wi-Fi, como el nombre de la conexión SSID y también la contraseña con su tipo de encriptación.

3

Podremos configurar el balance de brillo, si se trata de una cámara para interior o exterior, así como también ajustar los niveles de brillo y nitidez. Lo más importante es que nos permitirá configurar la luz eléctrica que ilumina la zona que estamos vigilando.

4

Desde la misma pestaña de configuración de imagen, podemos activar la visualización para dispositivos móviles. Algunas cámaras tienen la opción **Habilitar 3GP**, que es el formato de video que utilizaban los primeros dispositivos móviles.

Real-time IP Camera Monitoring System

Device Info
Alias Settings
Date & Time Settings
Users Settings
Multi-Device Settings
Basic Network Settings
Wireless LAN Settings
ADSL Settings
UPnP Settings
DDNS Service Settings
Mail Service Settings
FTP Service Settings
Alarm Service Settings
Upgrade Device Firmware
Restore Factory Settings
Reboot Device
Back

DDNS Service Settings

DDNS Service: DynDns.org(dynDNS) ▼

DDNS User: _____

DDNS Password: _____

DDNS Host: _____

DDNS or Proxy Server: _____

DDNS or Proxy Port: _____

DDNS Status: No Active

Re-Update Ignoring All Errors: ☐ Never do this unless your hostname has been unblocked
primary config is needed if the device is in China, Mainland or HongKong

Submit Refresh

5

Setup

Basic
Image
Administration
Users
Options
Motion Detection
Status

Advanced (PnP, Basic) Port

Enable (For HTTP/Web connections) Back to Top

Port Number: 1024 (1024 - 65534)

RTSP Port: 554 (554, 1024-65535) Back to Top

RTP Data Port: 5000 (1024-65514; Even number only)

Max RTP Data Packet: 1400 bytes (400-1400)

Disable Back to Top

Video Address: 224 2 0 1

Video Port: 2240 (1024-65534; Even number only)

Audio Address: 224 2 0 1

Audio Port: 2242 (1024-65534; Even number only)

Time to Live: 10 hours (1 - 100)

6

Setup

Basic
Image
Administration
Users
Options
Motion Detection
Status

Service Provider: TZO Web Site

Domain Name: _____

E-Mail Address: _____

TZO Key: 666666

Update Period: Every 15 mins

Status: _____

Update Now

Disable Enable Disable (Discovery Only)

7

Users Settings

User	Password	Group
admin	*****	Administrator ▼
visitante	*****	Visitor ▼
viewer	*****	Operator ▼
noalla	*****	Visitor ▼
		Visitor ▼
		Visitor ▼
		Visitor ▼

Submit Refresh

Set Record Path: C:\Users\Public\Documents Browse...

Set AlarmRecord Path: C:\Users\Public\Documents Browse...

8

5

El servicio DDNS nos permitirá tener una dirección web, a la que podemos acceder sin importar si nuestra IP cambia (como sucede en los servicios ADSL). Debemos fijarnos si nuestra cámara es compatible con los servicios DDNS, y luego registramos en **dyndns.org**.

6

En la configuración, podemos configurar el puerto para visualizar la cámara, que por defecto es el puerto 80. Recordemos que, al cambiar el puerto, para acceder nuevamente a la configuración o visualizar la cámara debemos poner **IP:puerto**, o sea, al cambiar el puerto al 8080, debemos ingresar **192.168.1.120:8080**.

7

El servicio UPnP, descubre los dispositivos dentro de la red local, no conviene tenerlo activado, ya que en algunos casos permite acceder al dispositivo para realizar algunas modificaciones sencillas, que ponen en conocimiento y riesgo la seguridad de la cámaras.

8

En la creación de usuarios, aunque nosotros mismos seamos los únicos que tengamos acceso a la configuración total de las cámaras, conviene crearnos además un usuario básico para nosotros. En caso de que necesitemos ver la cámara remotamente, utilizaremos el usuario básico y no el administrador.



Instalación física de una cámara IP

En estas páginas, revisaremos los aspectos generales que es necesario tener en cuenta antes de definir la ubicación física de nuestras cámaras de seguridad y la forma adecuada de realizar la instalación.

Una vez realizada la configuración y luego de probar su conexión cableada o inalámbrica, estamos en condiciones de elegir el mejor lugar para su ubicación física. Recordemos que, si estamos utilizando una cámara con una lente especial, ya tenemos una distancia al objetivo que debemos respetar para no perder calidad de imagen.

Ubicación

La ubicación de nuestra cámara no debe estar condicionada por factores externos, salvo excepción mayor. Por ejemplo, si en el lugar adecuado que hemos elegido para la cámara no contamos con un enchufe cercano y, por esa razón, decidimos cambiarla de lugar a una nueva ubicación donde no tendremos la visualidad que queríamos lograr. Antes de esto, debemos buscar la solución que mejor se adapte para tener un enchufe



Al abrir la caja de la cámara debemos asegurarnos de que estén todos los accesorios incluidos.

donde lo necesitemos, incluso, si es necesario, llamaremos a un electricista para estar seguros de que no realizaremos ninguna mala conexión. En cambio, encontrar mucha humedad o pequeñas

filtraciones de agua en la superficie que habíamos elegido para ubicar la cámara será un factor que nos obligue a cambiarla de lugar. Otra alternativa, pero en este caso para cámaras cableadas por UTP, si contamos con un equipo **PoE** (*Power over Ethernet*), consiste en aprovechar el mismo cableado para la alimentación eléctrica de la cámara. Las cámaras que se utilizan en los sistemas DVR/NVR utilizan, por lo general, un cable especial, que, además del cable para la señal de video, incluye otros dos cables que son de tensión y, como están fabricados para tal fin, pueden abarcar grandes distancias sin pérdida de amperaje. El transformador de la cámara tiene dos partes, la entrada de tensión y la salida de tensión. La salida de tensión



Cajas protectoras

Cuando instalamos nuestras cámaras, queremos estar seguros de que nada, tanto actos de personas como factores climáticos, las podrá romper. En un ambiente interno, resulta muy raro que se rompa una cámara, pero es muy distinto con las cámaras exteriores, que están desprotegidas. Para tal caso, existen cajas cerradas, con una ventana para la lente, que la protegen de la lluvia. Para una mayor protección, una práctica recomendada es ubicarlas lo más alto posible y que tengan una buena lente, para obtener una resolución óptima del lugar por visualizar.

es la que alimentará a la cámara para su funcionamiento. En caso de que no dispongamos de un enchufe cercano, no se debe alterar el largo del cable.

Visión

Antes de proceder a marcar el lugar fijo donde irá la cámara, debemos probar la visualidad que nos daría la cámara en ese lugar. Para eso, la dejaremos apoyada sobre una base cercana o provisoria, que armemos para tal fin, y, desde nuestra PC, nos conectaremos a ella para evaluar si el ángulo de visión es el adecuado que estamos buscando. Al realizar esto, nos daremos cuenta de diversos factores que hayamos pasado por alto, que pueden afectar a la visualidad de la cámara. Algunos de esos factores pueden corregirse sin cambiar la ubicación de la cámara, y otros no, como por ejemplo mucha luminosidad, lo que nos hará revisar la ubicación y buscar otra más adecuada. Esta tarea puede resultar monótona y repetitiva, pero debemos realizarla para obtener un mejor resultado.

Instalación

Si se trata de la instalación de nuestra propia cámara, no es conveniente dejarla apoyada sobre una plataforma, aunque esto nos resulte cómodo; jamás debemos confiarnos en que no se moverá, o que nadie la va a tocar en ese lugar.

En cambio, es necesario elegir un sitio no llamativo y que, a la vez, no sea de fácil acceso. Por ejemplo, si ponemos una cámara IP en un garaje, lo ideal sería fijarla en el techo, unos metros hacia dentro y en el medio, para tener visión, incluso, de la entrada cerrada; si la entrada es abierta, también se protegerá la cámara de las lluvias. Con esto nos aseguraremos de que, si alguien desea tocarla, deberá utilizar una escalera y llamará la atención; en cambio, si la dejamos apoyada sobre una plataforma, cualquier movimiento intencional o no podría dejarla fuera de visión.

Soporte

Una vez elegida la posición de la cámara, debemos colocar su soporte; este deberá estar amurado a la pared o al techo mediante tarugos para fijar su posición. Para ello, necesitaremos realizar cuatro orificios con un taladro. Empezaremos la instalación por la base de nuestra cámara y, con marcador indeleble, señalaremos el lugar donde va a ir colocada y la posición de los orificios, para luego ayudarnos a realizar los agujeros. En los agujeros



Con los ajustes de presión, podemos adaptar la posición de la cámara prácticamente en cualquier lugar.

realizados debemos colocar unos tarugos, que vienen en distintas medidas; tanto los orificios que realicemos como los tarugos y los tornillos que vayamos a utilizar tienen que ser de dimensiones compatibles. Junto con los accesorios que vienen en la caja de la cámara, se incluyen tornillos para fijar la base; lo recomendable es utilizar tornillos más largos, sobre todo si colocaremos la cámara en el techo.

Ajustes

Una vez que hayamos fijado la base, colocaremos la cámara. Tengamos en cuenta que la cámara trae dos ajustes a presión; uno de ellos nos permitirá ajustarla con respecto a la base. En este punto, el ángulo de la cámara con respecto a la base estará fijo, pero la cámara podrá rotar 360° grados. Con el otro ajuste a presión que generalmente se encuentra detrás de la cámara, ajustaremos la posición relativa de giro de la cámara con respecto a la visión que deseemos obtener, o sea, si la base está fijada desde el techo, entonces la cámara tendrá que estar en la posición contraria a la base para que, al ser visualizada desde nuestra navegador, no obtengamos una imagen invertida. Recordemos que las cámaras PTZ tienen la base fija a la misma cámara; cuando fijamos este tipo de cámara desde una posición lateral o vertical, en su configuración tendremos una opción que nos permitirá girar, rotar, espejar o invertir el sentido de la imagen visualizada. ■

Caja metálica de protección para aquellas cámaras que colocaremos en exteriores desprotegidos.





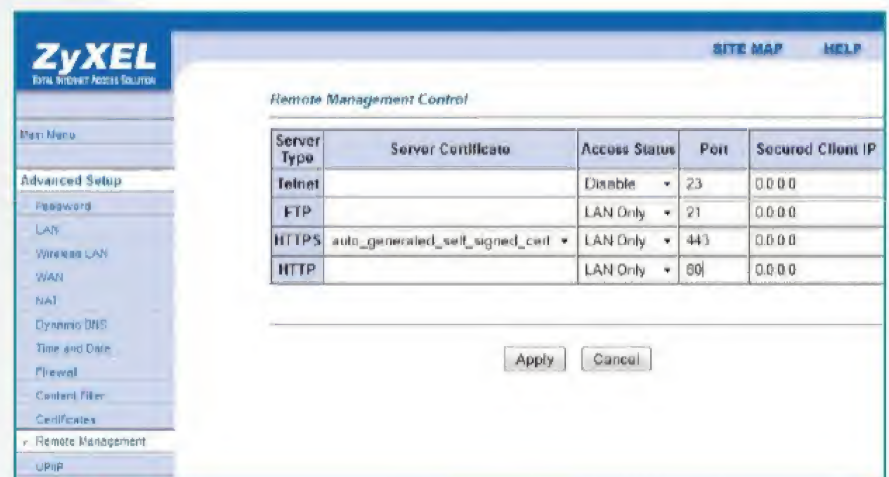
Configuración de un router Wi-Fi

En esta sección, conoceremos los detalles para configurar un router Wi-Fi; de esta forma, podremos monitorear las cámaras de seguridad a través de Internet en forma remota.

Para poder acceder a la cámara desde nuestra PC o smartphone dentro de la red local, deben estar configurados todos los dispositivos con direcciones IP que pertenezcan al rango. Además, debemos prestar atención a la conexión con la cámara IP. Si desde nuestra PC vemos la cámara, pero la imagen se congela aleatoriamente o nos aparece algún mensaje en el que se nos avisa que la página no fue encontrada, tal vez no se trate de un problema específico de la cámara o de su configuración, sino que la distancia entre la cámara IP y el router Wi-Fi es muy grande, o hay obstáculos, en el medio, que provocan pequeñas interferencias en la conexión. Una solución es poner un access point más cercano o cambiar la antena del router Wi-Fi por otra que nos dé un mayor alcance.

Puerto de visualización

Al visualizar la cámara, si no hemos modificado el puerto de visualización, no tendremos que realizar modificaciones en el router. Recordemos que, para ingresar a la página de configuración del router y de la cámara IP, solo debemos poner la IP del dispositivo en nuestro navegador y, como el puerto por defecto es el 80, no debemos ingresarlo. Si hemos cambiado el puerto de la cámara, debemos ingresarlo cada vez que deseemos visualizarla. Mientras nos encontremos dentro de la red local, hayamos modificado o no los puertos, no tendremos problemas para visualizar la



En esta imagen vemos la pantalla de configuración para el acceso remoto de nuestro router; aquí solo elegimos qué servicio habilitar.

cámara. Para acceder a la cámara desde Internet, o sea, en forma remota, debemos configurar el router para que entienda cómo procesar lo que deseamos visualizar. El router principal, si está configurado con los datos de nuestro proveedor ISP, tendrá dos IP, una privada que usamos en nuestra red local, y una pública, que es la que nos asignará nuestro ISP. Cuando nos conectemos remotamente, utilizaremos la IP asignada por nuestro ISP. Si estamos utilizando una PC y queremos ver la cámara de entrada de nuestra casa, pero ingresamos la IP que el ISP asignó a nuestro router y no podemos ver ninguna página, esto se deberá a cómo hayamos configurado nuestro router.

Opciones adicionales de configuración

Durante la configuración de nuestro router, habremos habilitado o denegado su configuración remota, sea a través del navegador web, telnet, o FTP. Si hemos habilitado la administración remota vía web, cuando queramos acceder a nuestra red remotamente, veremos la página de configuración de nuestro router como si estuviésemos en la red local. Esto se debe a que estamos utilizando el puerto 80.

Acceso remoto

Cuando accedemos remotamente al router para visualizar un equipo específico, en este caso nuestra cámara IP, debemos

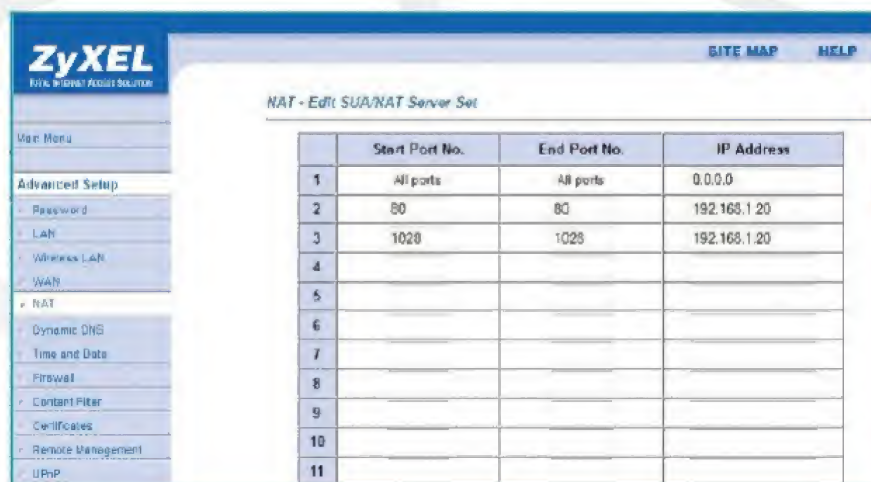
configurarlo. Podemos imaginar a nuestro router como un guía de tránsito; cuando llegamos a él y pedimos para ver nuestra cámara, no puede ayudarnos porque no tiene la información sobre tal dispositivo. Para poder ver la cámara IP, debemos configurar el router a través de un redireccionamiento de puertos.

Acceso remoto con acceso denegado al router

Como dijimos, ambos equipos (router y cámara IP) utilizan el puerto 80. Entonces, debemos configurar de tal forma que el router pueda interpretar lo que deseamos hacer. Una opción es configurar el acceso remoto del router a un nivel de seguridad solo local, y, a través del redireccionamiento de puertos, cuando se intente acceder remotamente al puerto 80, configuraremos el router para que desvíe el tráfico hacia la IP de nuestra cámara. Para ello, en la configuración de nuestro router, en la pestaña que dirá SUA/NAT o simplemente NAT, crearemos una nueva regla. Dependiendo del modelo de router, nos dejará ponerle un nombre a la regla de direccionamiento que nos permitirá recordar por qué razón la hemos creado. En este caso, redireccionaremos el puerto 80 hacia la IP privada de nuestra cámara IP. Con esta configuración, el router interpretará todas las peticiones remotas que se hagan al puerto 80.

Acceso remoto con acceso habilitado al router

Si deseamos poder tener acceso a la configuración del router y a la cámara IP simultáneamente, debemos configurar el router para permitir dicha tarea. En primer lugar, debemos cambiar el puerto de escucha al router o a la cámara IP. Lo aconsejable es cambiar el puerto al router, ya que esto le pondría un nivel de seguridad mayor, y, además, al dejar el puerto 80 como fijo para la cámara IP, podremos acceder a ella de manera rápida. En la configuración de NAT del router, dejaremos la regla de direccionamiento del puerto 80 apuntando a la cámara IP. Pero, en la pestaña de administración remota del router, habilitaremos la opción de configuración vía web, y permitiremos



ZyXEL
FIREWALL PORTAL SOLUTION

SITE MAP HELP

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	80	80	192.168.1.20
3	1020	1020	192.168.1.20
4			
5			
6			
7			
8			
9			
10			
11			

Podemos configurar el direccionamiento de puertos no solo para ver la cámara, sino incluso para otros servicios, como Escritorio remoto o streaming de video.

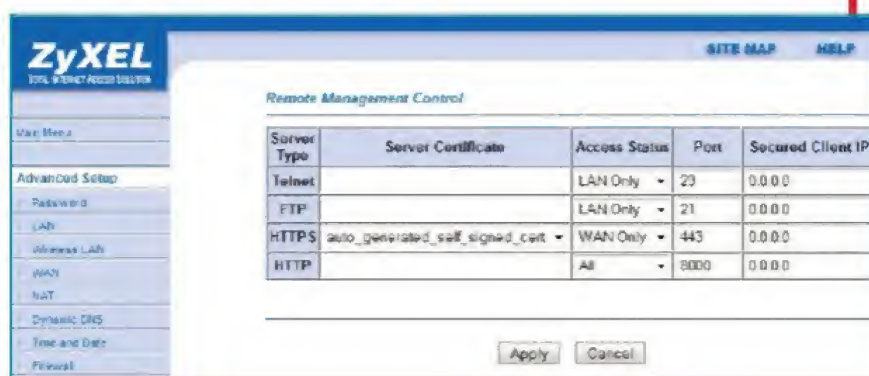
el acceso total, es decir, podremos acceder a la configuración del router tanto local como remotamente en el puerto especificado.

Acceso remoto a varias cámaras

Cuando disponemos de dos o más cámaras independientes, es decir, sin un sistema centralizado de vigilancia, cada cámara tendrá un puerto específico, y el direccionamiento de puertos es inevitable. El procedimiento es el mismo, solo que tendremos que evaluar cuál es para nosotros la cámara más importante; a esa le dejaremos el puerto 80 para facilitar el acceso a ella, mientras que, a la cámara secundaria, podemos configurarle el puerto 8080 y, al router, el puerto 8000. Aquellas cámaras que tienen una opción especial para su visualización en dispositivos móviles utilizan un puerto alternativo para tal modo. Este

puerto también lo debemos incluir en la tabla de direccionamiento del router. Entonces, si utilizamos un dispositivo móvil, podemos configurarlo para ver la cámara principal por el puerto 80 y la segunda cámara a través del puerto específico para dispositivos móviles. Hay cámaras que, en su configuración, prevén la utilización de más cámaras, e incluyen una opción para agregarlas dentro de la suya, de forma tal que, cuando visualizamos esa cámara, podemos también ver las otras, sin haber instalado ningún software especial. ■

En la configuración del router, es posible cambiar el puerto para su configuración. Debemos probar qué puerto está libre.



ZyXEL
FIREWALL PORTAL SOLUTION

SITE MAP HELP

Remote Management Control

Server Type	Server Certificate	Access Status	Port	Secured Client IP
Telnet		LAN Only	23	0.0.0.0
FTP		LAN Only	21	0.0.0.0
HTTPS	auto_generated_self_signed_cert	WAN Only	443	0.0.0.0
HTTP		All	8000	0.0.0.0

Apply Cancel



Administración de cámaras IP

La administración de las cámaras IP puede ser realizada en forma local o remota; en estas páginas, conoceremos la manera de llevarla a cabo.

Real-time IP Camera Monitoring System

Basic Network Settings

Obtain IP from DHCP Server ☐

IP Addr: 192.168.1.21

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS Server: 192.168.1.1

Http Port: 80

Submit Refresh

1

Real-time IP Camera Monitoring System

Date & Time Settings

Device Clock Time: Mon, 01 de abril de 2011 22:00:06

Device Clock Timezone: (GMT-03:00) Buenos Aires, Georgetown

Sync with NTP Server: ☒

NTP Server: time.mil.gov

Sync with PC Time: ☒

Submit Refresh

2

My Account

Create Account

LOGIN

Logout

Sign in to DynECT Managed DNS

Sign in to DynECT Email Delivery

Create an account or log in to continue

Username: _____

Password: _____

Confirm password: _____

Email: _____

Confirm Email: _____

Security Image:

Enter the numbers from the above image: _____

Subscribe to Dyn newsletter (one or two per month)

I accept the terms of Dyn's [Acceptable Use Policy](#), the [Dyn Services Agreement](#), and Dyn's [Privacy Policy](#)

Create Account

3

ZyXEL

Dynamic DNS

Active

Service Provider: WWW.DynDNS.ORG

Host Name: camaradejavier.dyn dns.org

Email Address: javier@gmail.com

User: tecnicojaviernadina

Password: *****

Enable WebCam

Apply Cancel

4

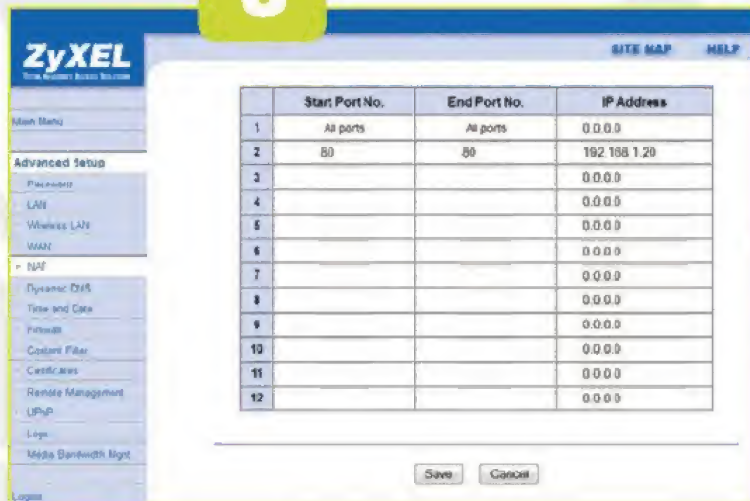
1 Para una mejor administración local, a las cámaras que agreguemos, les asignaremos un número consecutivo de IP, para acceder con facilidad a ellas a través de nuestro navegador de Internet y llevar un mejor control de los dispositivos que tenemos conectados a nuestra red.

2 Tenemos que revisar semanalmente la configuración de la cámara, y, según el modelo de cámara, se nos permitirá realizar un backup, que guardaremos en una carpeta específica. Si experimentamos cortes de luz, debemos revisar en cuanto se reintegre el servicio, si la hora y la fecha son correctas.

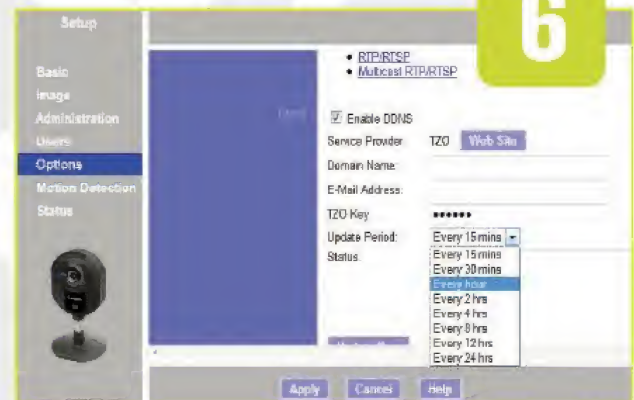
3 Para acceder a la cámara de forma remota sin memorizar nuestra IP pública (que además puede cambiar), debemos registrarnos y crear una cuenta en **DynDNS.org**. Podemos activar los 14 días de prueba del servicio y, al finalizar la prueba, solo podremos tener de forma gratuita un host.

4 Luego de crear el hostname en DynDNS, podemos configurar el router o la cámara con estos datos. Conviene configurar el router por si necesitamos acceder en forma remota, como cambiar un puerto o agregar una regla que hayamos olvidado.

5



6



7



8

5 Como el router y la cámara usan el puerto 80, configuramos el puerto 800 u otro para acceder al router, y el 80 redireccionado a la cámara, de forma que, si queremos acceder a ella, escribiremos la dirección del hostname creada en DDNS, y, si queremos acceder al router, escribiremos la misma dirección agregando :800 al final.

6 Algunos routers o cámaras soportan DynDNS.org e incluyen otros proveedores similares para usar exclusivamente con sus productos. Estos proveedores, a veces, no ofrecen una alternativa gratuita, o, si la tienen, esta caduca después de un determinado tiempo.

7 Una alternativa es utilizar No-IP. Para el servicio gratuito, descargaremos desde www.noip.com el cliente, que consiste en una aplicación, para la cual crearemos un nombre de usuario y contraseña, y luego podemos agregarle un hostname. Para que la IP se actualice, debemos dejar encendida la PC.

8 Usando No-IP, o DynDNS, podemos acceder a la configuración completa de nuestro router o cámara. Lo recomendable, al usar una PC que no es nuestra, es evitar loguearnos como administrador, y, si lo tenemos que hacer en un caso de urgencia, debemos habilitar la navegación privada.



Configuración adicional de cámaras IP

En esta sección configuraremos una cámara IP para recibir alertas ante eventos detectados y actualizar el firmware, entre otras tareas.

Las empresas que tienen monitoreado cada uno de sus sectores contratan a otra empresa prestadora de servicios de seguridad para vigilar y controlar el monitoreo en forma constante. Si nosotros disponemos de una o de pocas cámaras de seguridad para nuestro hogar y, además, no podemos estar vigilándola durante las 24 horas por nuestras actividades diarias, podemos configurar nuestra cámara para que nos envíe alertas por e-mail, o realizar una programación para que, en determinados horarios, se realice una grabación.

Alertas por FTP

Si contamos con un servicio de FTP propio o contratado, podemos configurar la cámara IP para que las imágenes o la grabación sean subidas en forma automática al servidor FTP. Para ello, en la opción de configuración del servicio FTP de la cámara, debemos ingresar la dirección IP de nuestro servidor FTP, el nombre de

usuario y su contraseña, el puerto utilizado, y en qué carpeta deseamos que se guarden los archivos. Conviene utilizar esta función si trabajamos casi constantemente con el servidor FTP, para tener alguna alerta visual desde la PC que estamos utilizando.

Alertas por e-mail

Una excelente opción son las alertas por e-mail. Podemos configurar que nos lleguen e-mails con imágenes instantáneas

En las alertas por e-mail, agregamos las cuentas a las que llegarán las notificaciones.

cada determinado tiempo o, lo más adecuado es configurar la recepción de e-mails cuando se detecta algún movimiento. La configuración para recibir las alertas por e-mail es muy similar a



Cámaras y luminosidad

Algunas cámaras tienen la opción de visión nocturna por medio de LEDs infrarrojos. Aun así, la calidad de imagen puede que no sea la que nosotros deseamos. Si queremos contar con una buena luminosidad cuando la cámara detecte movimiento, en aquellos modelos que cuentan con opción para activar alarmas podemos conectar un pequeño relé para que accione las luces que queramos y, en la configuración de la cámara, activar la opción de alarma. Esta opción está prevista por el fabricante, por eso en el manual encontraremos la información y las medidas de seguridad para su realización. Si nuestra cámara no cuenta con un conector para alarmas, podemos instalar un hardware externo, detector de movimiento, que activará las luces.

la configuración que realizamos en nuestro cliente de correo: debemos ingresar todas las configuraciones del servidor de correo saliente, usuario y contraseña, servidor SMTP, etc. Si utilizamos un correo gratuito, debemos comprobar que nos permita enviar varios e-mails, ya que los correos salientes de la cámara pueden ser considerados como envío masivo de e-mail, spam, y se nos bloquea temporalmente el servicio para el envío de e-mails en general. Lo que podemos hacer es registrar una cuenta gratuita, que nos permita utilizar los servicios POP3 y SMTP, y que utilizaremos exclusivamente para los servicios de nuestra cámara para configurar que las alertas por e-mail lleguen a ambas cuentas, a la que hemos creado para tal fin y a la que usamos en forma regular, de manera que cuando borremos los mensajes, siempre nos quedará una copia en la otra cuenta de correo. Algunas cámaras permitirán el envío únicamente a un destinatario, mientras que otros modelos permiten el envío a varios destinatarios, con lo cual, si queremos que todos los miembros de la familia reciban la alerta por e-mails, podemos hacerlo, o incluso configurar la cuenta de nuestro trabajo para recibirlos. Dependiendo de la cantidad de mensajes recibidos, es posible que nuestro cliente de correo considere la dirección de e-mail como spam; para evitar esta situación, debemos agregar la dirección a la lista de correo confiable.

Programación automática

Otra opción que podemos utilizar es la programación automática de grabación de video o tomas de fotografías simultáneas cada determinado tiempo o en un horario específico. Esta característica dependerá exclusivamente del modelo de cámara IP que tengamos. Para su configuración, iremos a la sección Alarm o Schedule. Si no la encontramos, deberemos consultar el manual de nuestra cámara para ver si tenemos dicha función. Debemos asegurarnos de que, en la configuración inicial de la cámara, hemos configurado correctamente la fecha y la hora. En la configuración de programación, debemos seleccionar

Es posible configurar que se graben los videos en horarios específicos.

Si tenemos servidor FTP, los registros se pueden cargar de manera automática.

la carpeta de nuestra PC en donde queremos que se almacenen los videos o las fotografías que la cámara registre. También configuraremos la opción para que los registros sean borrados de manera automática cada determinado tiempo o si se llega a un límite específico.

Actualización de firmware

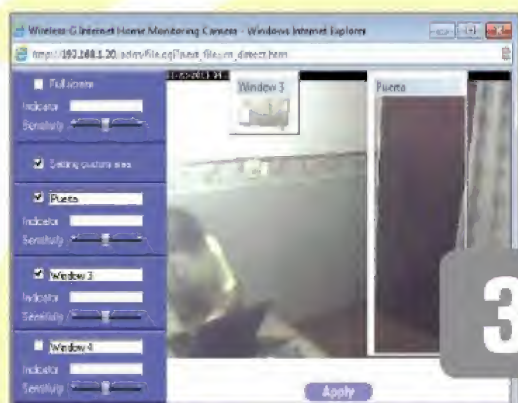
La actualización de firmware, por lo general se realiza para corregir algunos errores que puedan haberse encontrado en la cámara, o incluir nuevas funciones. Para aplicarla, debemos conectar nuestra cámara a la PC por medio del cable de red Ethernet. Luego de configurar la dirección IP de nuestra PC, ingresaremos a la

cámara como lo hacemos habitualmente, e iremos a la configuración avanzada; allí, se nos pedirá nuestro usuario y contraseña de usuario avanzado. Antes de realizar la actualización, podemos hacer un backup de la configuración actual. Hacemos clic en Update Firmware, buscamos el archivo con extensión .BIN que habíamos descargado antes y esperamos para seguir los pasos que irán apareciendo en pantalla. Es probable que, luego de la actualización, debamos ingresar con la IP y el usuario que vienen por defecto en la cámara. Si la actualización contiene algunas nuevas funciones, deberemos configurarlas, y ya estará funcional otra vez. ■



Configuración de la detección de movimiento

En estas páginas, configuraremos la alerta de detección de movimiento para diferentes modelos de cámaras.

**1**

En Configuración avanzada o en la opción Detección de movimiento, activamos la casilla de verificación para habilitar esta función. Nos dará a elegir qué opción deseamos ante la detección de movimiento: tomar fotografías o grabar el video, y el intervalo entre la detección de movimientos.

2

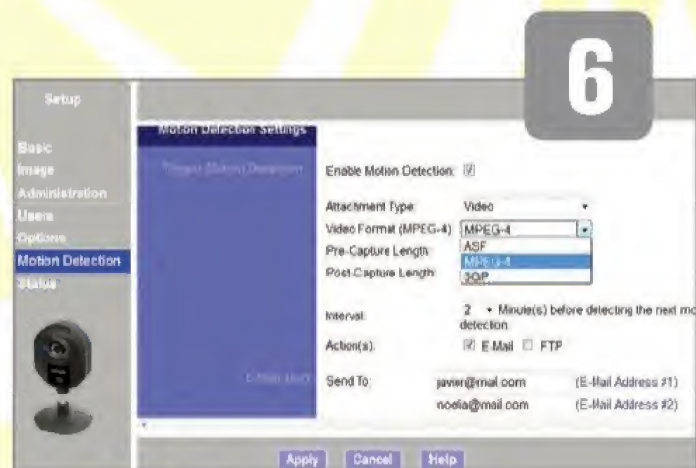
Si estamos la mayor parte del tiempo lejos del lugar donde se ubica la cámara, la mejor opción es activar el envío de imágenes por e-mail, ya que ocuparán poco espacio, y las podremos recibir, por ejemplo, en nuestro smartphone.

3

Según el modelo, podemos configurar las zonas que consideramos sensibles al movimiento. En cámaras exteriores, debemos tener en cuenta si tenemos mascotas, o árboles que puedan moverse con el viento y activar falsas alertas. Nuestras zonas sensibles, de toda la visión, son las puertas y las ventanas.

4

Las cámaras que no cuentan con la selección de una zona de sensibilidad, incluyen una opción global de sensibilidad para toda al área que abarca la visión de la cámara. Este tipo de cámaras son ideales para ubicaciones internas.



5 Podemos configurar que, además de que las imágenes nos lleguen por e-mail, sean subidas en forma automática a un servidor FTP. Para configurar el servidor FTP, nos pedirá la dirección, usuario y contraseña, y la carpeta donde queremos que se guarden los registros.

6 Si configuramos la cámara para la grabación de video, nos permitirá elegir el tipo de formato en el que queremos que sean grabados. Seleccionaremos según la calidad que deseamos obtener y el espacio del que dispongamos para guardar las grabaciones.

7 Si contamos con cámaras analógicas, podemos utilizar hardware especial de vigilancia para redes, en este caso de AirLive, en el que conectaremos nuestra cámara analógica y el servidor de video a nuestra red mediante cable. Otra opción, es conectar el AirLive a un sensor de movimiento.

8 Algunos modelos de cámara incluyen una ranura para tarjetas de memoria, en la que se guardarán los registros que hayamos configurado. Este tipo de cámaras es muy útil si solemos tener problemas de conexión con nuestro proveedor de Internet.



Monitoreo y grabación de imágenes

En estas páginas, conoceremos los detalles relacionados con la configuración de las cámaras IP, para que podamos realizar el monitoreo y la grabación desde distintos equipos.

Cuando disponemos de más de una cámara, incluso de varias cámaras para un mismo lugar enfocadas desde distintos puntos de vista, deseamos verlas todas simultáneamente en un mismo monitor, tomar fotografías o grabar los registros en su totalidad.

Debemos tener en cuenta que la actividad de esta función es similar a los CCTV, DVR o NVR dedicados.

Software GeoVision

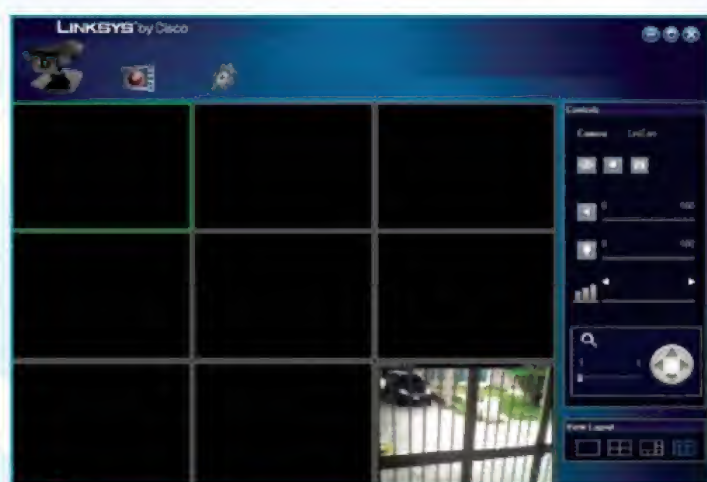
Si disponemos de varias cámaras con conexión coaxial o queremos adaptar un viejo sistema CCTV a nuestra PC, podemos utilizar las placas de GeoVision, que nos permiten conectar hasta 16 cámaras, y cuatro de ellas con audio.

Además, instalaremos el software de GeoVision, en el cual podemos configurar de qué cámaras queremos grabaciones durante las 24 horas; de cuáles en un horario determinado;

cuáles que solo tomen fotografías cuando se detecta movimiento; el formato de grabación, y el acceso remoto para visualizar las cámaras. Cuando lo configuramos, podemos decidir cuánto tiempo estarán almacenados los registros en nuestra PC, para que sean eliminados en forma automática por el mismo software. Debemos prestar atención a esta configuración para evitar quedarnos sin espacio en nuestro disco duro.

Software Linksys

Las cámaras fabricadas por Linksys incluyen el software **Wireless Internet Home Monitoring Camera**, que nos permite visualizar todas las cámaras que tengamos instaladas en nuestro hogar, oficina, etc. Al ser un software propietario, no nos permite agregar otras cámaras que no sean de la familia Linksys. El software buscará automáticamente todas las cámaras Linksys que encuentre en la red. Si no localiza ninguna, la podemos agregar en forma manual con su IP y especificar el puerto si es que lo hemos cambiado. Podemos configurar la grabación, para que se ejecute de manera automática, o configurando cuántas horas de video, o por capacidad, hasta cuántos GB se pueden grabar.



El software de Linksys (**Wireless Internet Home Monitoring Camera**) es gratuito y compatible con los productos proporcionados por esta empresa.

AL VIGILAR UN MISMO SITIO DESDE DISTINTOS ÁNGULOS, PODEMOS ALTERNAR UTILIZANDO CÁMARAS DE MAYOR O MENOR CALIDAD.

La programación automática, nos permitirá grabar en días y horarios específicos, o configurar que se grabe determinada cantidad de minutos cuando se detecte movimiento. Con este software podemos ver 1, 4, 6 o 9 cámaras simultáneamente. Al configurar las cámaras en forma individual, les pusimos un nombre identificador, como "Entrada garaje", "Patio", "Puerta principal"; es importante el hecho de ponerle a cada cámara un nombre que nos permita identificar, con rapidez, el lugar físico que estamos visualizando.

Cuando el espacio que hemos asignado para los registros se llena, el software de Linksys no nos provee una opción para eliminarlos, sino que nos dejará sobrescribir en los registros más viejos, o detener la grabación hasta que manualmente borremos los archivos de la carpeta en la que establecimos que se guardarían.

Security Monitor Pro

Desde www.deskshare.com, podemos descargar **Security Monitor Pro**. Básicamente su funcionamiento es similar al proporcionado por Linksys, pero, al ser una empresa desarrolladora independiente, nos permitirá agregar cámaras de distintos fabricantes para su visualización simultánea, con las que podremos controlar hasta 32 cámaras, lo que lo hace ideal para conectarla a un TV LCD de un gran tamaño.

Cada vez que agreguemos una cámara, debemos configurar una opción para la detección de movimiento; puede ser: notificación por e-mail, comienzo de la grabación del video, reproducción de un sonido en la PC, subida del video grabado a un servidor FTP, o ejecución de un programa determinado.

Una característica muy importante es que, independientemente de la configuración individual de cada cámara que hayamos agregado, podemos configurar la zona sensible para la detección de movimientos, pero al revés de la forma en que lo hemos realizado; en este caso, veremos la imagen completa que toma la cámara seleccionada, y, en vez de seleccionar nuestra zona sensible al movimiento, tenemos que marcar qué zonas deben ser ignoradas al movimiento para evitar falsas alarmas. Podemos configurar una o todas las cámaras para retransmitir la imagen visualizada, a través de la opción **Broadcast**. Para visualizarla desde otro equipo dentro de la red local, utilizaremos Windows Media Player, ingresando la IP de la PC en la que instalamos el software y el puerto según lo hayamos configurado en el software (este puerto es distinto del configurado en la cámara). Para poder acceder a la visualización de la cámara desde una ubicación remota, debemos configurar el router para

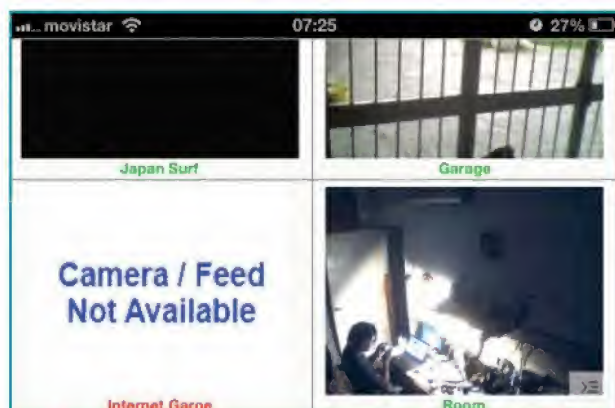


Placa PCI de GeoVision, que nos permite adaptar y convertir un CCTV en NVR.

el redireccionamiento de puertos. Debido a que al habilitar el broadcast de las cámaras para su visualización no se nos pedirá una contraseña, para una mayor seguridad solo conviene que lo habilitemos para aquellas cámaras principales, como las de entrada, sala de espera, o recepción; si queremos habilitar todas las cámaras porque la ubicación de la PC queda aislada, debemos prestar atención a la configuración de seguridad del router para que nadie ajeno pueda modificar sus parámetros. Al igual que los demás, este software incluye la opción para la programación automática; además, cuenta con un foro dedicado en la misma página del fabricante, con lo cual cualquier duda que tengamos sobre su configuración antes de adquirirlo o luego de hacerlo, podemos consultarla directamente por ese medio.

Monitoreo desde equipos móviles

Si deseamos ver nuestras cámaras desde una tablet o un smartphone, una aplicación ideal para estos equipos es **IP Cam Viewer**, que viene en su versión gratuita Lite y en la versión paga. Cuando nos conectamos de forma local, solo debemos ingresar la IP de cada cámara y seleccionar el modelo correcto; incluso si nuestra cámara no está listada en los modelos, podemos probar con la opción genérica. Si queremos visualizar las cámaras desde un punto remoto, debe estar configurado el router para el redireccionamiento de puertos, y, cuando agregamos la IP de nuestra cámara, ingresaremos la IP pública de nuestro router. Si deseamos ver más de dos cámaras al mismo tiempo desde nuestro equipos, tenemos que configurar distintos puertos para cada cámara; esto es posible realizarlo si nuestra conexión para subida es medianamente alta. Lo recomendable es que agreguemos todas las cámaras para su visualización local, cuando estamos dentro de la misma red, y dejemos una cámara para su visualización remota. Agregaremos dos veces la cámara que deseamos ver local y remotamente, una vez con la IP local, y la otra con la IP pública y el puerto configurado. ■



Con **IP Cam Viewer**, podemos visualizar las cámaras desde un smartphone. Su versión gratuita es algo limitada.



Seguridad y cámaras de monitoreo

En este apartado, revisaremos las características de las principales vulnerabilidades de los sistemas de seguridad.

Todas las cámaras, sin importar sus modelos, están expuestas a correr riesgo de diferentes tipos de inseguridad; para evitar caer en algunos de ellos, conoceremos las fallas más comunes que se producen cuando las instalamos. Esto nos indica que debemos estar atentos al modo de efectuar la instalación, tanto física como lógica.

Precauciones generales

Una de las precauciones que debemos tener al momento de fijar las cámaras es no dejar expuestos los cables de alimentación o cableado; lo ideal sería que estos cables fueran por tuberías internas o que contaran con canaletas protectoras externas. La ubicación de la cámara no debe estar expuesta al alcance de cualquier persona que pueda modificar su ángulo de visión;

si por razones de fuerza mayor la cámara quedara expuesta, entonces debemos colocarla dentro de una caja protectora. Cuando configuramos la cámara, debemos tratar en lo posible de modificar los parámetros que vinieron por defecto, en especial, no dejar ninguna contraseña por defecto y, si es posible, cambiar el nombre del usuario **Admin**, para ingresar a la configuración avanzada de nuestras cámaras.

Corte de servicios

Puede ocurrir que nos quedemos sin algún servicio, como luz, o conexión a Internet, por problemas técnicos o a causa de una actividad malintencionada. En esta situación, todos los equipos quedarían sin conexión a Internet o sin luz en toda la instalación.

Para poder alimentar los equipos, si utilizamos una PC como servidor, podemos usar UPS; según el modelo que adquiramos, podemos contar con una autonomía de electricidad que puede ir de pocos minutos a varias horas de duración. Según nuestra necesidad, elegiremos cuál se adapta mejor.

AL FIJAR LA CÁMARA NO DEBEMOS DEJAR EXPUESTO NINGÚN TIPO DE CABLE.

En el caso de la suspensión del servicio de Internet, si accedemos a las cámaras remotamente, podemos contar con un dispositivo de alarma complejo, que incluye una célula GSM; esta se puede configurar para que, al detectar la falta de un servicio (luz o Internet), se comunique automáticamente a través de mensajes de texto, para determinar qué acción realizar (por ejemplo, activar alarma sonora). Una configuración práctica de este conjunto consiste en conectar nuestras cámaras principales a un sistema UPS, y estas, o alguna de ellas, a su vez, a la alarma con GSM, de manera que, si nos quedamos sin ambos servicios y queremos acceder en forma remota para ver la cámara, podemos hacerlo.

Ataques de jamming

Los inhibidores o bloqueadores de señal son utilizados por los servicios de inteligencia y los grupos de seguridad:





Bloqueador de señal de celulares. Su uso sin licencia puede estar prohibido y se aplican importantes multas a su dueño.

su comercialización está regulada por la ley de cada país, como también su venta y permisos de uso. Estos dispositivos pueden bloquear, interferir o captar cualquier señal inalámbrica modificando su frecuencia, o sea, se ven afectadas las señales de celular, GPS, bluetooth y Wi-Fi. Aplicado a las cámaras de seguridad, un inhibidor de señal, nos dejará sin visualización de alguna de nuestras cámaras. Aquellas aplicaciones o equipos dedicados de vigilancia nos permiten configurar una acción ante la pérdida de señal de una cámara, que puede incluir desde emitir un sonido de alerta o encender luces hasta enviar mensajes de texto en los equipos más sofisticados.

Ataques físicos

Las cámaras externas son las más expuestas a recibir ataques físicos no solo intencionados, sino también debido al estado del tiempo. Los ataques intencionados tratarán de dañar la lente o la cámara en sí, por medio de golpes, pintura o algún otro elemento. Contra estos tipos de ataque, solo podemos tratar de mejorar la seguridad perimetral de la cámara; en ambientes abiertos, es posible utilizar alambres de púas, aumentar la distancia de posición de la cámara o utilizar cámaras que simulan ser luces exteriores.

Cámaras falsas

Existen dispositivos imitadores de seguridad, que sirven para distraer en caso de ataques externos o, incluso, para proteger la ubicación de las cámaras verdaderas. Estos equipos tienen todo el aspecto de ser una cámara de seguridad, con sus respectivos cables, y hasta pueden conectarse a la red eléctrica para simular una detección de movimiento, o sea, al detectar movimiento siguen a la fuente que lo generó. Una configuración típica es ubicar la cámara falsa en un lugar visible, pero de difícil acceso, mientras que las verdaderas cámaras se encuentran empotradas en la pared o en distintos ángulos que ofrezcan la visión general del lugar, protegidas por la distracción que ofrecen los dispositivos falsos.

Vulnerabilidades generales

Las vulnerabilidades son agujeros de seguridad que no fueron previstos por el fabricante durante la producción. Se pueden distinguir dos tipos: fallas de hardware o de software. Las fallas por hardware, prácticamente no tienen solución, ya que se trata de una falla en el diseño del chip, y la única alternativa es reemplazar la cámara; las fallas por software se pueden solucionar con la actualización del firmware o de la interfaz web que utilizamos para configurar la cámara. Es recomendable, cada cierto tiempo, revisar foros de Internet de usuarios de modelos de nuestras cámaras, como también si el fabricante ha liberado nuevos firmware. Los riesgos que se corren es que quedan expuestas las configuraciones, incluso, se pueden obtener las contraseñas de las configuraciones que hemos realizado, como e-mail y servidor FTP.

Descuidos en DVR

Un típico error en los sistemas DVR/NVR es utilizar el mismo monitor por el cual estamos visualizando todas las cámaras, para ver grabaciones anteriores. Cuando estamos viendo grabaciones viejas, por el motivo que sea, al retirarnos debemos asegurarnos de que volvimos a dejar la imagen en modo de tiempo real. Si dejamos reproduciendo una grabación anterior, en la que se registra el ingreso de personas que desconocemos, puede provocar una falsa alarma a las autoridades, y, por el contrario, si la grabación es una repetición de rutina diaria, quedamos expuestos a que intenten ingresar personas no autorizadas a nuestro sector, sin que lo notemos. Salvo que la situación lo requiera, es mejor ver



Cámara falsa. Su diseño la hace prácticamente imposible de distinguirse de una real.



Distribuidor VGA. Permite transmitir la señal VGA a través de la red hasta 150 metros sin repetidor.

los videos grabados a contrahorario, o, si se han cargado a otro medio –un servidor FTP por ejemplo– visualizarlos directamente desde ahí, y dejar el monitor del sistema DVR para su visualización en tiempo real.

Seguridad física del NVR

El lugar donde tengamos centralizado el sistema de monitoreo debería ser poco accesible al público en general. El NVR lleva, en su interior, uno o dos discos duros de gran capacidad para las grabaciones diarias. Aunque pongamos el NVR en un lugar seguro, del cual no pueda ser retirado por varias personas, igual está expuesto a recibir golpes que dañen el disco duro. Como el NVR dispone de conexión a Ethernet, para la mayor seguridad de las grabaciones podemos conectar al mismo router a un NAS (*Network Attached Storage*). En el NVR, configuraremos que las grabaciones se copien al NAS simultáneamente, y ubicaremos el NAS en un lugar escondido, como un techo falso, un panel falso de electricidad, etc. De esta forma, nos aseguramos de que, en caso de que se quiera dañar al

NVR, quedará una copia hasta antes del incidente en cuestión, entregándonos la posibilidad de saber qué acción se realizó justo antes de ocurrido el incidente de seguridad.

Consideraciones finales

Como hemos analizado en este fascículo, la instalación y correcta configuración de un sistema de vigilancia basado en cámaras IP nos provee de diversas ventajas, muchas de ellas son evidentes, como el aumento en el nivel de seguridad en los sectores vigilados, pero también existen algunas ventajas ocultas, como la reducción en forma drástica de la necesidad de contar con personal de seguridad, en el caso de que la instalación se efectúe en una pequeña empresa. También la posibilidad de cubrir áreas más extensas, optimizando, de esta forma, el trabajo de vigilancia.

Otro de los aspectos importantes por destacar es la disuasión, ya que un sistema de cámaras de seguridad se encarga de prevenir y evitar la ocurrencia de incidentes de seguridad con su sola presencia, disuadiendo a los posibles ladrones. No podemos dejar de mencionar a las cámaras de seguridad como un método de evidencia, ya que almacenan grabaciones que se pueden considerar pruebas de cualquier robo o acción

LAS MODIFICACIONES QUE SE REALICEN EN LA CONFIGURACIÓN DE SEGURIDAD DEBEN HACERSE MIENTRAS UTILIZAMOS LA NAVEGACIÓN PRIVADA.

delictiva, las cuales podrán ser utilizadas como evidencia en un juicio o acción legal en contra de los responsables. Finalmente, es importante destacar que las cámaras IP mejorarán la efectividad y procedimientos relacionados con el control y la supervisión continua de la seguridad; de esta forma, los empleados trabajarán de manera más eficiente. Así, en caso de presentarse errores en la producción, el sistema de cámaras de seguridad permite revisar y determinar sus causas. ■

¿TE RESULTA ÚTIL?

Lo que estás leyendo es el fruto del **trabajo de cientos de personas** que ponen todo de sí para lograr un **mejor producto**. Utilizar versiones "**pirata**" desalienta la inversión y da lugar a publicaciones de **menor calidad**.

NO ATENTES CONTRA LA LECTURA. NO ATENTES CONTRA TI. COMPRA SÓLO PRODUCTOS ORIGINALES.

Nuestras publicaciones se comercializan en kioscos o puestos de voceadores; librerías; locales cerrados; supermercados e internet (usershop.redusers.com). Si tienes alguna duda, comentario o quieres saber más, puedes contactarnos por medio de usershop@redusers.com

CONVIÉRTETE EN UN
EXPERTO CON LA COLECCIÓN:

**SALIDA
LABORAL**

TÉCNICO en ELECTRÓNICA

CONCEPTOS FUNDAMENTALES Y PRÁCTICA PROFESIONAL

CON ESTA COLECCIÓN PODREMOS:

- ▶ ENTENDER LOS CONCEPTOS CLAVES DE ELECTRICIDAD Y ELECTRÓNICA.
- ▶ UTILIZAR LOS INSTRUMENTOS DE MEDICIÓN DE LABORATORIO.
- ▶ SIMULAR, CONSTRUIR Y MEDIR CIRCUITOS.
- ▶ CONTROLAR DISPOSITIVOS DE MANERA INALÁMBRICA.
- ▶ APROVECHAR AL MÁXIMO SENSORES Y TRANSDUCTORES.
- ▶ UTILIZAR LA PLATAFORMA ARDUINO.



ESTA OBRA INCLUYE:

24 fascículos + 4 libros + 3 eBooks + 1 coleccionador

BIBLIOTECA DIGITAL



Nuestro catálogo listo para
leer en PC o iPad



¡LEELO COMO
QUIERAS!

Ahora puedes acceder
a los libros USERS a
través de Internet,
no más esperas ni
problemas de envío

¡LEELO DONDE
QUIERAS!

Con la calidad de
siempre, abarcando los
temas del momento,
incorporando servicios
complementarios y
pagando menos

NUEVAS ediciones a



Accede a un libro de muestra www.redusers.com/u/2hq



9 789871 857784

ACCEDER A LA BIBLIOTECA DIGITAL **USERS**



usershop.redusers.com



+54(011)4110-8700



usershop@redusers.com